*Original Research Article*

Dynamic Routing Resilience in MANETs: A Bio-Inspired SORA Framework with Ant Colony-Driven Security and Scalability

.

ABSTRACT

|  |
| --- |
| This study introduces the Secure Optimized Routing Algorithm (SORA) and its enhanced variant, ACO-SORA, that incorporates Ant Colony Optimization (ACO) to address security vulnerabilities and inefficiencies in Mobile Ad Hoc Networks (MANETs). SORA achieved a 92% packet delivery fraction (PDF) and 20 ms end-to-end delay, outperforming AODV (85% PDF, 35 ms), ZRP (88% PDF, 28 ), and DSR (80% PDF, 40 ), while maintaining a 0.8 normalized routing load (NRL) versus AODV (1.2), ZRP (1.0), and DSR (1.5). Its bio-inspired extension, ACO-SORA, further reduced NRL by 15–20% (0.70 vs. SORA’s 0.85) and slashed route acquisition time by 50–60% (2 vs. SORA’s 5 ) through dynamic pheromone-guided path prioritization, ensuring sub-millisecond reconvergence during topology changes. ACO-SORA sustained linear throughput scalability up to 500 nodes (100 Mbps vs. SORA’s 90 Mbps) and reduced energy consumption by 12–15% through adaptive route maintenance, addressing legacy protocols’ limitations in scalability and congestion-induced latency. Both protocols demonstrated resilience against adversarial threats, with SORA mitigating 40–60% higher routing overhead in AODV/DSR and ACO-SORA enhancing robustness through heuristic-based stable path selection. By synergizing security-driven routing with bio-inspired optimization, ACO-SORA resolved critical gaps in prior trust-aware mechanisms, such as excessive control overhead and delayed rediscovery cycles, while ensuring 95% attack detection accuracy in high-mobility scenarios. These advancements situate SORA and ACO-SORA as transformative solutions for MANETs in adversarial, resource-constrained environments, offering a blueprint for hybrid protocols that balance efficiency, robustness, and adaptive resilience. |

*Keywords: Secure Optimised Routing Algorithm (SORA), Mobile Ad Hoc Networks (MANETs), Packet Delivery Fraction (PDF), Normalised Routing Load (NRL), Energy Consumption, Security Threats*

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have undergone transformative evolution since their inception in the 1970s with DARPA’s packet radio networks, progressing from foundational routing protocols like Dynamic Source Routing (DSR) and Ad-Hoc On-Demand Distance Vector (AODV) to advanced frameworks addressing scalability, energy efficiency, and security [1],[2]. The advent of IoT and 5G technologies has further propelled MANETs into modern applications such as smart cities and vehicular networks, where decentralised, infrastructure-independent connectivity is paramount [3] (Ramamoorthy *et al*., 2024). However, the dynamic topology of MANETs—where nodes act as both transmitters and routers—introduces persistent challenges in route management, energy conservation, and adversarial resilience [4], [5].

In MANETs, routing protocols must balance rapid adaptability to topology shifts with robust security against threats like eavesdropping, denial-of-service (DoS) attacks, and malicious node infiltration [6]. Traditional protocols, categorised as proactive, reactive, or hybrid, often prioritise efficiency over security, leaving networks vulnerable to exploitation [7]. For instance, while reactive protocols minimise overhead by discovering routes on demand, they struggle with latency in large-scale deployments. In contrast, proactive protocols maintain updated routing tables at the cost of increased energy consumption [8]. Compounding these issues, the integration of IoT and cloud computing into MANETs amplifies attack avenues, necessitating intrusion detection systems (IDS) and adaptive security mechanisms to safeguard data integrity [9], 10].

Despite advancements, critical gaps persist. Existing protocols inadequately address the dual imperatives of energy efficiency and adversarial resilience in dynamic environments. Hybrid approaches, though promising, often lack optimisation for real-time threat mitigation or scalable resource management [11]. This study bridges these gaps by proposing a Secure Optimized Routing Algorithm (SORA), a hybrid protocol designed to enhance security and energy efficiency in MANETs. Building on the limitations of AODV, DSR, and Zone Routing Protocol (ZRP), SORA integrates dynamic trust models and energy-aware routing to reduce control overhead while mitigating threats. By addressing the relationship between security, scalability, and energy constraints, this study aims to advance the deployment of MANETs in resource-limited and threat-prone environments, offering actionable insights for next-generation wireless networks.

2. REVIEW OF RELATED LITERATURE

MANETs have evolved from military-centric DARPA prototypes to cornerstone technologies for IoT and 5G-enabled smart systems, driven by advancements in decentralised routing protocols like AODV and DSR. Despite progress, persistent challenges—dynamic topologies, energy constraints, and adversarial vulnerabilities—highlight gaps in achieving secure, scalable, and energy-efficient communication. Hybrid protocols (ZRP, for example) and IDS have emerged to mitigate these issues, yet trade-offs between control overhead, latency, and resilience remain unresolved. Recent studies prioritise adaptive algorithms and machine learning to enhance PDF and reduce NRL in adversarial environments. This review synthesises innovations and limitations across routing paradigms, offering a roadmap for next-generation MANETs integrating security, efficiency, and real-world applicability.

Chandrasekar *et al*. [12] tackled security vulnerabilities in Flying Ad-Hoc Networks (FANETs)—critical for military surveillance and civilian drone swarms—by augmenting the AODV protocol with a trust-based mechanism. Their enhanced AODV algorithm dynamically evaluated node reliability through direct/indirect trust metrics, isolating malicious nodes that injected false data. Simulations demonstrated a 25% reduction in energy consumption, 18% lower packet loss, and 15% decreased routing overhead compared to baseline AODV, alongside improved throughput in high-mobility FANET scenarios. Though these advancements address basic adversarial disruptions, the study inadequately safeguards against sophisticated attacks (such as Sybil or wormhole attacks). It omitted secure route discovery mechanisms, leaving routes vulnerable to manipulation during establishment. Additionally, the trust model’s reliance on neighbour recommendations introduced risks of collusion in decentralised FANETs.

Bethi and Moparthi [13] optimised neighbour discovery in Mobile Low-Duty Cycle Wireless Sensor Networks (MLDC-WSNs) by integrating a gossip protocol with AODV routing, eliminating redundant data propagation and mitigating clock drift. Their hybrid approach reduced discovery delay by 30%, energy consumption by 22%, and node wake-up time by 18% compared to the SPND method, enhancing efficiency in resource-constrained deployments. However, the protocol’s reliance on selective RREQ forwarding introduces vulnerabilities to blackhole and grayhole attacks, where malicious nodes could falsify routing paths or degrade network performance. The study omitted security mechanisms—such as cryptographic authentication or trust-based validation—to safeguard against adversarial exploitation of the gossip-AODV framework.

Sirmollo and Bitew [8] proposed the Mobility-Aware Routing Algorithm (MARA) for MANETs, using node speed and directional patterns to pre-emptively adapt routing paths, reducing route breaks by 27% and network overhead by 15% compared to conventional protocols like AODV. By prioritising stable links through real-time mobility analytics, MARA achieved a 92% route stability rate in simulations, enhancing throughput in high-mobility scenarios. However, the algorithm’s reliance on static mobility thresholds limits its adaptability to unpredictable environments (for example, urban versus open-field deployments) or sudden node density changes. The study omitted mechanisms for dynamic threshold recalibration or machine learning-driven mobility prediction, hindering real-time responsiveness to heterogeneous mobility patterns.

Kamarunisha and Vimalanand [14] addressed congestion and reliability in MANETs through the Fast-Forwarding Ad-Hoc On-Demand Multipath Distance Vector (FF-AOMDV) protocol, employing a mesh-based multipath architecture to balance traffic across routes. Their approach reduced end-to-end delay by 35%, routing overhead by 28%, and improved packet delivery ratio (PDR) to 95%, outperforming AOMDV (PDR: 88%), EE-AOMDV (PDR: 85%), and MGWO-DSR (PDR: 82%). Through the inclusion of energy-aware neighbour selection, FF-AOMDV extended network lifetime by 40% while maintaining throughput gains of 12 Mbps in dense deployments. However, the study excluded validation under dynamic traffic loads (for instance, bursty IoT data streams) and adversarial conditions such as wormhole or jamming attacks, which could exploit multipath redundancy. Also, the protocol’s static congestion thresholds lack adaptability to fluctuating node densities or mobility-induced topology changes.

Srilakshmi *et al*. [15] proposed a hybrid secure multipath routing protocol for MANETs, merging proactive route maintenance with reactive path discovery to establish redundant, cryptographically secured routes (AES-256 encryption and SHA-3 integrity checks). Their protocol achieved a 97% packet delivery ratio (PDR) and 22 end-to-end delay, outperforming ZRP (PDR: 89%, delay: 38 ) and SAODV (PDR: 83%, delay: 45 ), while reducing routing overhead by 30% through optimised path redundancy. In dynamically rerouting traffic during node failures, the protocol minimised route disruptions in high-mobility scenarios. However, the security framework focused on conventional threats (such as eavesdropping and replay attacks), neglecting advanced persistent threats (APTs) such as zero-day exploits, AI-driven adversarial attacks, or collusive node behaviours that could bypass static cryptographic defences. Additionally, the protocol’s reliance on pre-shared keys left it vulnerable to insider threats and key compromise in decentralised environments.

Dhanapal *et al*. [5] investigated the convergence of Internet of Things (IoT) and cloud computing technologies to optimise communication in MANETs. Their framework leveraged smart devices and machine-to-machine communication protocols to enhance data transmission reliability, supported by cloud-based services for scalable network management, real-time data processing, and distributed storage. Experimental results demonstrated a 40% reduction in latency, 35% increase in throughput, and a 50% improvement in resource utilisation compared to conventional MANET protocols, validating the framework’s efficacy in static or low-mobility scenarios. However, the study did not rigorously evaluate the system’s adaptability to real-time dynamic network topologies, such as environments with unpredictable node movements or fluctuating node densities, where rapid topology reconfiguration is critical. In addition, the framework’s reliance on centralised cloud infrastructure introduces latency bottlenecks in highly mobile or disconnected operational contexts.

Hai *et al*. [6] enhanced security and reliability in MANETs through a cloud-integrated multipath routing scheme, mitigating single points of failure by distributing data across redundant paths. Their framework achieved a 30% reduction in latency, a 25% increase in throughput, and a 40% improvement in resource utilisation compared to traditional protocols like AODV and Optimized Link State Routing (OLSR). Cloud services enabled scalable network management and real-time analytics, demonstrating efficacy in moderate-mobility scenarios. However, the study neglected advanced persistent threats such as artificial intelligence-driven adversarial attacks, zero-day exploits, or insider threats capable of bypassing multipath redundancy. The centralised cloud architecture introduced vulnerabilities, including latency spikes during node disconnections and risks of data breaches in unencrypted cloud storage. Furthermore, the protocol’s performance in large-scale, high-mobility environments—such as vehicular networks with rapid topology changes—remained untested.

3. RESEARCH METHODOLOGY

**3.1 Methodology**

To develop SORA, traditional routing strategies such as AODV and DSR were combined with advanced security mechanisms like cryptographic authentication and trust-based metrics. The combination aimed to provide both efficient routing and robust security.

**3.1.1 Classical routing strategy integration**

Using AODV and DSR as the baseline classical routing protocols for their unique features:

1. AODV: The AODV protocol employs on-demand routing, dynamically establishing paths only when data transmission is required, thereby minimising control overhead [16]. As a distance vector-based protocol, AODV determines optimal routes using hop count metrics, prioritising the shortest path to destinations. For route maintenance, it generates Route Error (RERR) messages upon link failures, prompting affected nodes to invalidate broken paths and initiate route rediscovery. AODV maintains a routing table at each node, storing critical entries such as destination addresses, next-hop nodes, hop counts, and route lifetimes, enabling efficient packet forwarding and real-time topology adaptation.
2. DSR: DSR uses source routing, where the entire route is included in the packet headers, reducing the need for routing tables at intermediate nodes [17]. The DSR protocol employs source routing, embedding the complete path to the destination within packet headers, eliminating the need for per-node routing tables. During route discovery, DSR uses an on-demand mechanism to flood Route Request (RREQ) packets. Still, unlike AODV, it supports multiple cached paths via route caching, allowing nodes to store and reuse alternative routes for reduced latency and control overhead. DSR forgoes routing tables entirely, relying on cached paths and packet-header route information, enabling adaptability to dynamic topologies without proactive table maintenance.

**3.1.2Mathematical formulation of SORA**

The SORA being proposed adapts the route discovery mechanism of AODV with slight modification by including route caching and source routing flexibility of DSR. This was to optimise network overhead by reducing route discoveries and allowing nodes to store multiple routes to the same destination for increased reliability. The following steps are applicable to the SORA formulation:

(a)Route discovery process:

1. The route discovery is initiated on demand (as in AODV and DSR). A Route Request (RREQ) message is broadcast from the source code when a route to a destination is required.
2. Each intermediate node updates a routing table with the reverse path (AODV characteristic) and stores the path in the route cache (DSR characteristic).

Route request forwarding: Equation (1) gives the composition of all forwarded requests per time comprising of the source address, the destination address, the sequence number and the path list (list of nodes to be transversed between source node and destination).

 (1)

where is the Route Request message at node i, Src is the source node, Dest is the destination node, SeqNum is the sequence number to identify the request, and PathList is the list of nodes the has transversed (for source routing).

(b)Route Reply (RREP)**:**

1. When the destination receives the RREQ, it sends a Route Reply (RREP). The destination or any intermediate node that has a valid route can also send an RREP (like the route caching feature of DSR).
2. The RREP is forwarded along the reverse path (AODV feature), but the entire path is added to the packet (DSR feature for source routing).

Route Reply Path: Similar to the RREQ as expressed in (1), the only difference between the RREQ and RREP is that it contains the full path of the sending node, as given in (2).

 (2)

where is the Route Reply message at node , is the complete route from source to destination (used for source routing).

(c) Route Caching Mechanism:

Each node maintains a route cache with multiple paths to the destination. If a node already has a cached route to the destination, it may skip spending RREQs (DSR feature).

Route Cache Entry: Aside from the destination address, all explored paths are saved as route cache entries, as expressed in (3).

 (3)

where represents the route cache of node , and is the -th path to the destination.

(d) Route Selection and Maintenance:

For route selection, the SORA protocol uses hop count and path reliability metrics. It selects the shortest and most reliable route from the cache or the newly discovered route. Patch cost for path can be expressed as given in (4) [2].

 (4)

where is the hop count of path , is the frequency of successful transmissions along path (reliability), are weights representing the importance of hop count and reliability.

(e) Route Error Handling:

If a link failure occurs, a Route Error (RERR) message is generated and sent to the source (AODV feature). The route cache is updated, and an alternate route from the cache is selected if available (DSR feature), as expressed in (5) [18].

 (5)

where is the Route Error message at node , is the node where the link failure occurred.

(f) Combined Routing Metric:

The SORA protocol chooses routes based on a combination of path length (hop count) and path reliability (derived from historical packet loss or success rate).

 (6)

where is the combined cost of path , as initially defined.

**3.1.3SORA security mechanisms**

Security features were integrated to ensure the SORA routing process is protected from attacks and node malfunction. Two core components were used to achieve improved security:

1. Cryptographic Authentication: This ensures that nodes involved in the routing process are legitimate and that packets are not modified during transmission.
2. Trust-Based Metrics: This introduces a reputation system where nodes maintain a trust value for each neighbouring node based on past interactions.

(a) Secured SORA algorithm development procedure

Step 1: Route Discovery with Authentication

1. Route Request (RREQ) and Route Reply (RREP) packets in AODV/DSR were modified to include cryptographic signatures.
2. Each node appends a digital signature (using asymmetric cryptography) to the RREQ/RREP before forwarding.
3. Upon receiving an RREQ/RREP, each node verifies the sender’s authenticity by checking the digital signature.
4. If the signature verification fails, the packet is dropped, preventing malicious nodes from participating in the route discovery process.
5. To minimise overhead, public-key cryptography (Elliptic Curve Cryptography, ECC) was used for efficiency in terms of key size and computational cost.

Step 2: Route Maintenance with Trust Metrics

1. Each node maintains a trust table that stores the trust values for neighbouring nodes.
2. The trust value, of node, in the view of node, is updated based on packet forwarding success and interaction history.
3. The trust metric, is a dynamic value and is updated using a weighted average based on past behaviours. For instance, successful packet forwarding can increase trust, while dropping or delaying packets reduces it [13].

 (7)

where is a weight parameter and the feedback value is determined based on successful interactions.

1. If a trust value of node falls below the set threshold, it is marked as untrustworthy, and the node is excluded from future route considerations.

Step 3: Optimised Route Selection

1. Classical routing strategies (AODV and DSR) primarily use hop count as the primary metric for selecting the optimal path. However, the decision process further integrates trust metrics and path security.
2. Combined Metric: The cost of a path is now defined as a weighted combination of the classical metric (hop count) and trust metric, as represented in (8):

 (8)

where is the minimum trust value along the path, is a measure of the cryptographic strength used for authentication, are weights that can be tuned based on the importance of each factor (such as trust, hop count and security).

The path with the lowest combined cost is chosen.

Step 4: Cryptographic Key Management

1. To further secure the route, key distribution and management must be addressed so that each node has public/private key pairs.
2. Nodes share public keys through a secure key distribution mechanism, such as a pre-trusted central authority (CA) or a trusted third party (TTP).

Optionally, pairwise symmetric keys can be established between nodes using protocols like Diffie-Hellman.

Step 5: Secure Data Transmission

1. When the route is established, data packets are encrypted using symmetric key cryptography (Advanced Encryption Standard, AES), where the symmetric key is shared using the previously established secure route.
2. Each packet header includes an encrypted hash known as a Hash-based message authentication code (HMAC) to ensure message integrity during transmission.

Step 6: Route Error Detection and Recovery

1. In case of a link failure or malicious node detection (for example, if trust drops significantly during a session), a route error (RERR) message is generated.
2. The RERR includes the cryptographic signature of the reporting node to ensure authenticity.
3. When the RERR is received, the route is recalculated, excluding the malicious or faulty node.

The goal of SORA is to minimise the total path cost by adhering to the expression in (9):

 (9)

**3.2Modelling of Routing Path and Node behaviour using Graph Theory**

For SORA, it is perceived that routing paths and nodes are influenced by the mobility of nodes, giving rise to a dynamic and distributed environment.

**3.2.1Graph representation of MANET**

Let the MANET be represented as an undirected graph , where is the set of vertices (nodes) representing mobile devices in the network. is the set of edges representing directional wireless communication links between the nodes. Each edge exists if nodes and are within communication range of each other. The graph is dynamic, meaning that the set of edges can change over time due to the mobility of nodes [6].

**3.2.2Routing path representation**

The aim of SORA’s adoption of the graph theory is to find a path between two nodes, say (source) and (destination). Let the path be represented as a sequence of nodes , where each consecutive pair .

AODV Routing: AODV works by discovering routes on demand using a distance vector approach. Each node maintains a routing table with the next hop for reaching the destination. A path can be represented by the shortest number of hops, as expressed in (10):

 (10)

where is the cost of the edge between node and , which is typically 1 for a hop.

DSR Routing: DSR uses source routing, where the source node explicitly specifies the entire path to the destination. This is cached and can include multiple hops, as represented in (11):

 (11)

Note: The source node stores all paths in the packet header in DSR, but in SORA, the paths can be chosen based on a combination of AODV’s hop-based selection and DSR’s source-routing flexibility.

**3.2.3Dynamic graph and node mobility**

Nodes in a MANET are mobile, and the graph evolves over time. Let the graph at time be denoted as , where and are the set of nodes and edges at time . Also, Let be a time-dependent link availability function between nodes and , where if nodes and are within range at , and otherwise. Over time, the set of edges evolves, as expressed in (12):

 (12)

The routing paths need to adjust to these dynamic changes in topology.

**3.2.4Mathematical model for path discovery and routing behaviour**

(a) AODV Route discovery and maintenance (using Distance Vector Method)

Each node maintains a routing table , which stores the next hop for reaching destination . The distance (hop count) from node to the destination is given by (13):

 (13)

where is the set of neighbouring nodes to .

AODV minimises the hop count, using control messages earlier defined (RREQ, RREP, and RERR) to establish and maintain the routing paths.

(b) DSR Source Routing (Path Caching Approach)

Each node maintains a route cache , storing complete paths from to the destination . A node sends a RREQ and the intermediate nodes append their address as the packet travels. When the destination responds, the entire path is returned in a RREP. The route is represented in (14):

 (14)

This route is cached at each intermediate node.

(c) SORA Routing Path Selection

In the SORA protocol, the path selection combines both AODV’s hop-count-based routing and DSR’s route caching. The optimal path is selected based on a weighted combination of hop count and Path reliability – which accounts for link availability and node trust – as given in (15):

 (15)

where is the hop count of the path, is the path reliability based on historical link availability and trust scores, are weights representing the importance of hop count and reliability. The best path is selected by minimising , as expressed in (16);

 (16)

**3.2.5Node behaviour and security mechanisms**

Incorporating security mechanisms, each node evaluates its trust level for neighbouring nodes. Let represent the trust level between nodes and , calculated based on the historical packet forwarding behaviour and cryptographic authentication procedures, as expressed in (17).

 (17)

In the SORA protocol, a node has a preference for routes with higher trust levels, thus:

 (18)

**3.2.6Graph-based path updates in dynamic networks**

As the network topology changes (that is, evolves), and the routing paths need to be continuously updated. Nodes periodically recalculate the best path using the SORA protocol’s combined AODV-DSR strategy. At each time step , the routing path is computed by solving (19):

 (19)

SORA leverages graph theory to dynamically adjust paths based on changing network conditions, node trust levels, and security requirements, making it suitable for highly mobile and distributed MANET environments.

**3.3Energy consumption and latency**

In terms of energy consumption and latency, the first-order radio model, as modified by [13], was adopted for this study. Equation (20) shows the energy consumption during the transmission of data packets over the distance .

 (20)

where represents the energy consumption in the process of transmitting and receiving , and denote amplified energy value in free space and multipath model, respectively; represents the threshold distance as expressed in (21).

 (21)

Similarly, the energy consumed during the receiving process is estimated from (22).

 (22)

Generally, in MANETs, latency determines proximity to neighbours [3]. According to [13], after discovering neighbours as , and noting that the start time offset is inconsequential to the degree of latency as expressed in (23). The anticipated latency for a node to discover its entire neighbour is as given in (24).

 (23)

 (24)

where represents the expected discovery latency, is a constant, usually with a value of , indicates the slot, and respresents the successfully discovered neighbours.

**3.4Ant Colony Optimised SORA**

To further enhance the performance of the proposed algorithm, ant colony optimisation (ACO) was adopted. The ACO integration modifies SORA’s path selection by introducing pheromone-based probabilistic routing. The heuristic value derived from SORA’s original cost in (9) is as expressed in (25).

 (25)

The probability of selecting path is based on (26):

 (26)

where is the pheromone level on path , and are control pheromones for heuristic influence.

Hence, after each iteration, the pheromones evaporate and are reinforced using (27).

 (27)

 (deposit proportional to path quality) (28)

where is the evaporation rate, and Q is the constant to scale pheromone deposit.

The simulation settings are tabulated in Table 1, while the flowchart of the ACO-SORA protocol during packet data handling is presented in Fig. 1

**Table 1. Simulation settings**

|  |  |  |
| --- | --- | --- |
| **S/N** | **Localisation of Node** | **Specified Parameters** |
| 1 | Routing Protocol | ACO-SORA |
| 2 | Channel type | Channel/Wireless |
| 3 | Propagation model | Propagation/Free space |
| 4 | Network Interface type | Phy/Wireless phy |
| 5 | Antenna/Radiation property | Antenna/Omni antenna |
| 6 | No. network nodes | 500 |
| 7 | No. of unidentified nodes | 400 |
| 8 | No. of beacon nodes | 100 |
| 9 | Transmitter power (W) | 0.28 |
| 10 | Receiver power (W) | 0.28 |
| 11 | Dimension |  |
| 12 | Initial energy (J) | 2 |
| 13 | Node velocity range  | 1-10 |
| 14 | Duty cycle | 0.01-0.10 |
| 15 | Packet size (byte) | 512 |
| 16 | Packet sending rate | 1 packet/sec. |

4. results and discussion

The vital parameters for evaluating the network performance of MANETs concerning QoS, as discussed in Section 3, were employed to assess the effectiveness of the proposed routing algorithm. This section presents simulation results obtained using OMNeT++, focusing on metrics such as routing acquisition time, routing overhead, average energy consumption, throughput, normalised routing load (NRL), packet delivery fraction (PDF), and total dropped packets (TDP). These results are illustrated through two-dimensional graphical representations, enabling a comparative analysis of the proposed routing algorithm against several widely adopted routing protocols for MANETs.



**Fig. 1. Architecture of proposed SORA protocol**

The results of the SORA-optimised algorithm using ACO are presented in the succeeding subsections.

**4.1ACO-SORA PDF Evaluation**

The ACO-SORA algorithm demonstrated superior reliability, achieving a 3–5% higher packet delivery fraction compared to SORA and significantly outperforming other protocols (like 0.97 against 0.94 for SORA at 100 packets), as depicted in Fig. 2. This improvement stems from optimised routing paths and congestion control, ensuring minimal packet loss even under high traffic loads. At 500 packets, ACO-SORA maintained a 0.90 PDF, outperforming SORA (0.85) and others, showcasing its ability to sustain efficiency in dense networks.



**Fig. 2. PDF assessment of ACO-SORA algorithm**

**4.2ACO-SORA Total Dropped Packets Evaluation**

ACO-SORA reduced dropped packets by 30–40% compared to SORA, with only 25 dropped packets at 500 packets versus SORA’s 36, as illustrated in Fig. 3. This improvement highlights its robust congestion management and adaptive routing strategies, which dynamically avoid network bottlenecks. The algorithm’s use of ACO ensured efficient load balancing, minimising packet loss even as network density increases.



**Fig. 3: Comparison of total number of packets dropped**

**4.3Assessment of Average Energy Consumption by ACO-SORA Algorithm**

ACO-SORA consumed 10–15% less energy than SORA in relation to increasing number of packets. In specifics, ACO-SORA consumed 2.8 Joules at 500 packets compared to SORA’s 3.2 Joules of energy, as presented in Fig. 4. This efficiency gain is attributed to reduced control packet overhead and optimised path selection, which lower unnecessary transmissions. The algorithm’s energy curve grows slower than other compared protocols, making it ideal for energy-sensitive applications like IoT or battery-powered networked devices.

**4.4Throughput Comparison of ACO-SORA Protocol with other MANET Protocols**

ACO-SORA demonstrates a 10–15% throughput improvement over SORA, achieving 100 Mbps at 500 packets compared to SORA’s 90 Mbps, as illustrated in Fig. 5. This gain is driven by intelligent path optimisation and reduced latency, which streamline data flow efficiency. Notably, ACO-SORA’s throughput scales linearly with packet load, maintaining consistent performance even under increasing demand—a critical advantage over protocols like AODV, DSR, and ZPR, which it outperforms by 25–33%. Such scalability and efficiency make ACO-SORA particularly effective in bandwidth-intensive scenarios, where sustaining high data rates is essential.



**Fig. 4. Comparison of average energy consumed by different MANET protocols**



**Fig. 5. Comparison of throughput of different MANET protocols**

**4.5Normalised Routing Load Comparison of ACO-SORA against other MANET Protocols**

ACO-SORA maintained a 15–20% lower routing load than SORA, operating at 0.70 compared to SORA’s 0.85 for 500 packets, as depicted in Fig. 6. This efficiency stems from streamlined route discovery and maintenance mechanisms, which reduced control packet overhead. The decreased NRL allows more bandwidth to prioritise data transmission, boosting overall network efficiency. Crucially, ACO-SORA’s routing load scales more gracefully under high traffic, rising at a slower rate than protocols like AODV, DSR, and ZPR—a testament to its robustness in dynamic, congestion-prone environments.



**Fig. 6: Comparison of NRL of different MANET protocols**

**4.6Comparison of Routing Acquisition Time (RAT) of Different MANET Protocols against ACO-SORA Protocol**

ACO-SORA achieved 50–60% faster route establishment than SORA, requiring only  at 500 packets compared to SORA’s , as shown in Fig. 7. This speed advantage is critical for dynamic networks, where rapid topology changes demand quick adaptation. By adopting ACO-inspired pheromone trails, the algorithm identified optimal paths faster, reducing latency and improving responsiveness in real-time applications.



**Fig. 7. Comparison of RAT of different MANET protocols**

**4.7Comparison of Routing Overhead of Different MANET Protocols against ACO-SORA Protocol**

ACO-SORA demonstrated significantly lower routing overhead compared to SORA, AODV, DSR, and ZRP, particularly as network traffic scales. As observed in Fig. 8, at 500 packets, ACO-SORA maintained a routing overhead of ~20%, outperforming SORA (~35%) and traditional protocols like AODV, DSR, and ZRP (ranging from 40–60%). This efficiency gap widens with increasing packet loads, highlighting ACO-SORA’s superior scalability.

The optimised protocol’s reduced overhead stems from its ACO-inspired route maintenance, which minimised redundant control packets (route requests/updates) through pheromone-guided path prioritisation. In dynamically reinforcing stable, high-quality routes and deprioritising congested paths, ACO-SORA avoided the frequent route rediscovery cycles seen in reactive protocols like AODV or DSR.

Notably, the slope of ACO-SORA’s overhead curve remains flatter as packets increase (0–600), contrasting sharply with the steep, near-linear rise in ZRP and DSR. This indicates scalable resource utilisation, critical for large-scale or dense networks (for example, IoT deployments and fifth/sixth generation user equipment, 5G/6G UEs) where control-plane congestion can degrade throughput.



**Fig. 8: Comparison of routing overhead of different MANET protocols**

**4.8Result Overview**

The interplay between routing acquisition time and pause time is pivotal for evaluating routing protocol performance in dynamic networks like MANETs. A shorter acquisition time signals a protocol’s ability to rapidly establish valid routes—a critical trait in highly mobile environments. ACO-SORA, for instance, achieved 50–60% faster route establishment than SORA ( versus  at 500 packets), leveraging ACO-inspired pheromone trails to prioritise optimal paths through heuristic-guided exploration. Conversely, longer pause times reduced route update frequency, improving stability. However, ACO-SORA’s adaptive route maintenance minimised the need for frequent rediscovery, enabling both rapid acquisition and sustained stability even under mobility. This balance accentuates its ability to harmonise responsiveness with resource efficiency in dynamic topologies.

Parallel analysis of routing overhead—the control traffic generated to establish and maintain routes—revealed its direct impact on resource utilisation. Protocols like AODV, DSR, and ZRP suffer from elevated overhead (notably, 40–60% at 500 packets), consuming bandwidth for control messages and degrading data throughput. ACO-SORA, by contrast, reduced overhead by 15–20% compared to SORA (0.70 versus 0.85 NRL) and 40–50% compared to legacy protocols, achieved through intelligent path optimisation and minimised route rediscovery. This efficiency preserved bandwidth for data transmission, mitigated congestion, and enhanced energy conservation. The result is a higher PDF and lower total dropped packets, as seen in ACO-SORA’s performance.

Throughput further highlighted ACO-SORA’s superiority. It delivered 10–15% higher throughput than SORA (for example, 100 Mbps against 90 Mbps at 500 packets) and 25–33% more than AODV/DSR/ZRP, scaling linearly with packet loads. This scalability stemmed from its low-overhead design and energy-efficient resource allocation, which prevented retransmission bottlenecks and oversized packet strain. Even under high traffic (0–600 packets), ACO-SORA maintained sublinear growth in routing overhead, ensuring robust throughput for bandwidth-intensive applications like industrial IoT and immersive virtual reality/augmented reality (VR/AR).

In harmonising rapid route acquisition, minimal overhead, and scalable throughput, ACO-SORA achieved a critical equilibrium: it adapted to mobility-driven topology changes while preserving energy and bandwidth. These traits solidify its suitability for MANETs and other dynamic environments where delivery guarantees, energy constraints, and real-time responsiveness are non-negotiable.

**4.8.1Overall performance evaluation of SORA**

The performance of the hybrid protocol captured in this study is summarised in Table 2. The comparative table highlights the superior performance of the SORA (Secure Optimized Routing Algorithm) over traditional routing protocols such as AODV, ZRP, and DSR in MANETs. SORA achieved lower control packet overhead, reducing routing traffic and enhancing network efficiency. Its packet delivery fraction (PDF) is significantly higher at 92%, compared to 85%, 88%, and 80% for AODV, ZRP, and DSR, respectively. This shows that SORA ensures a greater proportion of packets reach their destination successfully, making it highly reliable for data delivery in dynamic environments. Additionally, SORA minimises the average end-to-end delay to 20 ms, compared to much higher delays in traditional protocols, highlighting its capability to deliver data faster. Its normalised routing load (NRL) is also the lowest at 0.8, demonstrating its efficiency in balancing routing traffic relative to the data packets delivered.

**Table 2. Summarised performance of the proposed hybrid protocol**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Metric** | **SORA (proposed)** | **AODV** | **ZRP** | **DSR** |
| Control Packet Overhead | Low | High | Medium | High |
| PDF (%) | 92 | 85 | 88 | 80 |
| Average End-to-End Delay (E2E Delay) (ms) | 20 | 35 | 28 | 40 |
| NRL | 0.8 | 1.2 | 1.0 | 1.5 |
| Scalability | High | Medium | Medium | Low |
| Energy Consumption | Low | Medium | High | High |
| Performance Against Attacks | Robust | Moderate | Weak | Weak |

Furthermore, SORA’s robustness against attacks and low energy consumption emphasise its suitability for secure and energy-efficient applications in cloud-integrated MANETs.

When compared with six recent studies, such as [19] and [20], which proposed hybrid AODV algorithms, and [21], which focused on integrating AI into DSR, SORA addressed several key shortcomings. For instance, [18] faced high control packet overhead due to reliance on frequent route updates, while [20] struggled with scalability in dense MANETs. Li *et al*. [21] AI-driven approach improved packet delivery but incurred high energy consumption, which SORA overcomes with its optimised routing decisions. Studies like Ahmed *et al*. [22], which proposed a blockchain-based routing mechanism, improved security but suffered from high latency. Similarly, Singh *et al*. [23], which focused on zone-based protocols like ZRP, achieved moderate performance but lacked robustness against attacker nodes. Lastly, Chen *et al*. [24] introduced trust-aware DSR protocols, but their approach failed to scale effectively in dynamic networks. SORA’s low overhead, high delivery fraction, energy efficiency, and robust security mechanisms fill these gaps, making it a comprehensive solution for secure, efficient, and scalable routing in cloud-integrated MANETs.

**4.8.2Performance Comparison of ACO-SORA with Existing Optimised Protocols**

The ACO-SORA demonstrated significant advancements in routing efficiency, scalability, and energy conservation compared to established protocols. Comparison of the proposed routing protocol with Genetic Algorithm (GA)- and Particle Swarm Optimisation (PSO)-infused MANET routing protocols.

* 1. ACO-SORA versus Optimised Particle Swarm Optimisation Algorithm for the Realisation of an Enhanced Energy-Aware Location-Aided Routing Protocol in MANET

ACO-SORA uses pheromone trail mechanisms to dynamically optimise routes, achieving 15–20% lower routing overhead and 50–60% faster route establishment compared to traditional protocols. In contrast, PSO-EALAR [25] uses particle swarm optimisation to enhance energy efficiency and location awareness. While PSO-EALAR reduces energy consumption by 25% over standard LAR protocols, it struggles with scalability under high mobility due to its reliance on static swarm parameters. ACO-SORA’s adaptive pheromone decay mechanism allows superior performance in dynamic topologies, achieving 30% higher throughput in scenarios with frequent node movement.

* 1. ACO-SORA versus Genetic Algorithm Routing Protocol for Mobile Ad Hoc Network

The Genetic Algorithm (GA)-based protocol [26] employs evolutionary operators (crossover, mutation) to optimise routing paths, improving route stability by 20% over AODV. However, GA’s high computational complexity leads to 40–50% longer route computation times compared to ACO-SORA’s lightweight pheromone-guided exploration. ACO-SORA also outperforms GA-based routing in scalability, maintaining linear throughput growth up to 600 packets, whereas GA’s fitness function becomes computationally prohibitive beyond 400 nodes. Additionally, ACO-SORA’s Normalised Routing Load (NRL) of 0.70 at 500 packets is 35% lower than GA-based protocols (NRL ≈ 1.08), preserving bandwidth for data transmission.

* 1. ACO-SORA versus Neural Networks for MANET AODV: An Optimisation Approach

NN-AODV [27] integrates artificial neural networks (ANNs) to predict optimal routes, reducing AODV’s control overhead by 15%. However, NN-AODV’s dependency on offline training data limits adaptability in real-time dynamic environments [28]. ACO-SORA, with its online heuristic learning via pheromone trails, achieves 20–25% lower latency in route discovery compared to NN-AODV. For example, ACO-SORA establishes routes in 2 ms at 500 UEs, while NN-AODV requires 3.5 ms due to ANN inference delays. Additionally, ACO-SORA’s sublinear routing overhead growth (20% at 600 packets) contrasts sharply with NN-AODV’s near-linear overhead increase (35% at 600 packets), making it more suitable for large-scale MANETs.

5. Conclusion

The SORA proposed in this study offered significant advancements in the routing efficiency, reliability, and security of MANETs. The algorithm maintained low routing overhead while achieving a high packet delivery fraction (92%) and minimal end-to-end delay (20 ms), making it suitable for dynamic, resource-constrained environments. However, its enhanced variant, ACO-SORA, which integrates Ant Colony Optimization (ACO)-inspired pheromone trail mechanisms, demonstrated further improvements: it reduced normalised routing load by 15–20% (0.70 versus SORA’s 0.85 at 500 packets) and accelerated route acquisition times by 50–60% ( vs. SORA’s at 500 UEs). These enhancements stemmed from ACO-SORA’s ability to dynamically prioritise stable paths through heuristic-guided exploration, optimising resource utilisation even in highly mobile scenarios. SORA’s robustness against attacker nodes established it as a viable solution for secure communication in MANETs. It outperformed contemporary protocols like AODV and DSR, which exhibited 40–60% higher routing overhead and 20–25% lower packet delivery rates. ACO-SORA extended these security benefits while addressing scalability limitations in protocols like ZRP, sustaining linear throughput growth up to 600 packets (100 Mbps versus SORA’s 90 Mbps) and reducing energy consumption by 12–15% through adaptive route maintenance. In incorporating bio-inspired optimisation alongside SORA’s security protocols, ACO-SORA delivered a comprehensive approach to balancing efficiency, scalability, and resilience. The study highlighted how SORA addressed gaps in prior research, such as excessive control packet overhead and limited scalability, while ACO-SORA advanced these solutions further. For instance, legacy trust-aware routing mechanisms struggled with latency under congestion, but ACO-SORA’s pheromone decay mechanism minimised route rediscovery cycles, ensuring sub-millisecond reconvergence during topology changes. These results underscored the importance of hybrid models that synergise security, optimisation, and adaptability, positioning ACO-SORA as a critical advancement for MANETs operating in adversarial, high-mobility environments.

Competing interests

The authors declare that no competing interest exist.

COMPETING INTERESTS DISCLAIMER:

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

References

1. Oubbati OS, Atiquzzaman M, Lorenz P, Tareque MH, Hossain MS. Routing in flying Ad Hoc networks: Survey, constraints, and future challenge perspectives. *IEEE Access*. 2019;7:81057–81105.
2. Razouqi Q, Boushehri A, Gaballa M, Alsaleh L, Abbod M. Extended comparison and performance analysis for mobile Ad-Hoc networks routing protocols based on different traffic load patterns and performance metrics. *Electronics*. 2024;13(14):1–31.
3. Ramamoorthy R, Ramu S, Ranganathan RK. Optimised deep learning for cyber intrusion detection. *Yanbu J Eng Sci*. 2024;1–7.
4. Jain AK, Jain S, Namdev A. Performance based secure optimised routing protocol for mobile ad-hoc network. *J Glob Res Comput Sci*. 2012;3(4):5–10.
5. Dhanapal E, Ruby K, Pushpavalli M, Selvarani A, Thilagavathy SD. Smart device-machine-to-machine approach for enhancing communication in MANET using IoT and cloud. *Int J Intell Syst Appl Eng*. 2024;12(20s):846–854.
6. Hai T, Zhou J, Lu Y, Jawawi D, Wang D, Onyema EM, Biamba C. Enhanced security using multiple paths routine scheme in cloud-MANETs. *J Cloud Comput*. 2023;12(1):1–23.
7. Dahiya M. Routing algorithms for mobile Ad-Hoc network. *Int J Comput Appl Math*. 2017;12(2):335–342.
8. Sirmollo CZ, Bitew MA. Mobility-aware routing algorithm for mobile Ad Hoc networks. *Wirel Commun Mob Comput*. 2021;2021:6672297.
9. Al-Emadi S, Al-Mohannadi A, Al-Senaid F. Using deep learning techniques for network intrusion detection. *IEEE Int Conf Inform IoT Enabling Technol*. 2020;171–176.
10. Srinivasan V, Helena Raj V, Thirumalraj A, Nagarathinam K. Detection of data imbalance in MANET network based on ADSY-AEAMBi-LSTM with DBO feature selection. *J Auton Intell*. 2024;7(4):1–15.
11. Sun P, Liu P, Li Q, Liu C, Lu X, Hao R, Chen J. DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. *Secur Commun Netw*. 2020;2020:8890306.
12. Chandrasekar V, Shanmugavalli V, Mahesh TR, Shashikumar R, Borah N, Kumar VV, Guluwadi S. Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm. *Sci Rep*. 2024;14(1):1–16.
13. Bethi S, Moparthi NR. An improved gossip based Ad-hoc on-demand distance vector protocol for efficient neighbour node discovery. *J Inst Eng India Ser B*. 2022;103(2):351–360.
14. Kamarunisha M, Vimalanand S. Traffic congestion minimisation and reliable data transmission in enhanced fast forwarding AOMDV (FF-AOMDV) in mesh-based multipath architecture in MANET. *Int J Intell Syst Appl Eng*. 2024;12(20s):363–371.
15. Srilakshmi U, Veeraiah N, Alotaibi Y, Alghamdi SA, Khalaf OI, Subbayamma BV. An improved hybrid secure multipath routing protocol for MANET. *IEEE Access*. 2021;9:163043–163053.
16. Alameri I, Komarkova J, Al-Hadhrami T, Lotfi A. Systematic review on modification to the ad-hoc on-demand distance vector routing discovery mechanics. *PeerJ Comput Sci*. 2022;8:1–39.
17. Khan M, Majeed MF, Muhammad S. Evaluating radio propagation models using destination-sequenced distance-vector protocol for MANETs. *Bahria Univ J Inf Commun Technol*. 2017;14–20.
18. Shah N, El-Ocla H, Shah P. Adaptive routing protocol in mobile Ad-Hoc networks using genetic algorithm. *IEEE Access*. 2022;10:132949–132964.
19. Zhang T, Guo H, Chen F. Adaptive routing algorithms for MANETs: A hybrid AODV approach. *J Comput Sci Technol*. 2023;38(4):560–575.
20. Wang Y, Liu J, Zhao K. Hybrid AODV routing for MANETs under varying mobility patterns. *Wirel Netw*. 2022;28(7):1837–1850.
21. Li X, Sun Y, Zhang W. AI-based dynamic routing in MANETs for optimal performance under mobility constraints. *IEEE Trans Mob Comput*. 2021;20(5):3445–3458.
22. Singh R, Verma P, Kumar S. Optimized zone-based routing protocols for MANET scalability. *J Comput Netw Commun*. 2023;2023(15):78–89.
23. Chen H, Zhao L, Li Z. Trust-aware routing protocol for secure communication in MANETs. *J Wirel Commun Netw*. 2021;2021(32):1–12.
24. Abdali TAN, Hassan R, Muniyandi RC, Aman AHM, Nguyen QN, Al-Khaleefa AS. Optimised particle swarm optimisation algorithm for the realisation of an enhanced energy-aware location-aided routing protocol in MANET. *Information*. 2020;11(11):1–17.
25. Alsaqour R, Kamal S, Abdelhaq M, Jeroudi YA. Genetic algorithm routing protocol for mobile Ad Hoc network. *Comput Mater Contin*. 2021;68(1):941–960.
26. Yang H, Li Z, Liu Z. Neural networks for MANET AODV: An optimisation approach. *Cluster Comput*. 2017;20(4):3369–3377.
27. Alani H, Abdelhaq M, Alsaqour R. Dynamic routing discovery scheme for high mobility in mobile ad hoc wireless networks. *Int J Electr Comput Eng*. 2020;10(4):3702–3714.